ENGINEERING

CUTTING THE CORD FOR CLASSIFIED

Helping Customers Improve Service Quality, Save Money, and Meet Requirements for Assured Communications Using Commercial Wireless Devices and Networks

Efficiently operating commercial and government enterprises requires highly assured network communication. In severe environments, this was traditionally approached by utilizing wired networks to limit attacks, exfiltration, and impersonation – but this approach also limits interconnection, flexibility, and responsiveness. In this case study, we explore how implementing a wireless network –in compliance with the National Security Agency's (NSA) specifications for Commercial Solutions for Classified (CSfC) – allowed a customer to achieve high confidence in the protection of their communication, while also eliminating the cost and complexity of configuring and running a network with hardware encryptors.

THE CHALLENGE

A Peraton Labs' customer is routinely on the move with a set of shared commodity laptop computers that access a highly protected infrastructure network. To meet user requirements, the customer carries its laptops and specialized networking and encryption equipment to each new site. As the customer moves to a new location, technicians set up a wired network joining the laptops, encryption equipment, and a local router gateway to the infrastructure network. Because the laptops are shared among the personnel, each laptop is configured to connect to a Microsoft Active Directory server, enabling a new user to walk up to and use any workstation without a user-specific configuration change being required on the workstation.

- For customers requiring a high level of assurance in wireless communication, Peraton Labs designs solutions that meet the NSA specifications for carrying classified data over wireless networks.
- As an NSA-designated Trusted Integrator, Peraton Labs has the technology, experience, and certifications to design and implement integrated hardware and software solutions for assured communications across commercially available wireless devices.
- For more information on our CSfC integration services, see CSfC trusted integrator - Peraton Labs or contact trusted.csfc@mail.peratonlabs.com

While the existing solution delivered a secure communication capability, it carried an unacceptable cost in terms of the set-up time and the traveling weight of the cables and associated networking equipment. Additionally, each new location introduced potential troubleshooting costs as the physical network had to be repeatedly broken down and manually re-established, introducing opportunities for equipment failure and human error.

THE SOLUTION

Peraton Labs designed and implemented a wireless solution in compliance with the NSA Commercial Solutions for Classified (CSfC) program. CSfC is the NSA-approved process for using commercially available technologies to protect classified information. The program defines a path for NSA-designated Trusted Integrators to design, implement, and receive approval to operate qualified solutions that leverage commodity or commercial off-the-shelf (COTS) hardware and software products to carry classified communications.

In this case, after designing and implementing a COTS-based Wi-Fi solution to replace the copper network, Peraton Labs guided the customer through CSfC registration, integration exercises, and deployment.

Our customer had a goal of using low-cost, readily available commodity hardware to enable highly assured communication of classified data over an otherwise unprotected wireless network.

To achieve this goal, Peraton Labs defined target systems, components, and technologies and devised processes and configurations compatible with relevant CSfC capability packages. The Peraton Labs' solution provided an automated mechanism for converting standard Army Gold Master (AGM)-based systems from wired assets to wireless assets capable of and permitted to connect to Secret Internet Protocol Router–or SIPR–networks.

Peraton Labs delivered a fully CSfC-capable system compliant with NSA-defined Mobile Access Capability Package (MACP) for validation and subsequent use. Peraton Labs also designed a solution compliant with the NSA-defined Campus Wireless LAN (CWLAN) Capability Package.

THE RESULTS

Because Peraton Labs is recognized by NSA as a Trusted Integrator under the CSfC program, we were able to design and implement a highly assured wireless solution and obtain approval to operate it as a classified system.

The customer benefits of this solution include the ability to establish a mobile unit using COTS Wi-Fi products, supporting unmodified unicast and multicast classified IP traffic, and no longer needing to carry and configure a wired network to new tactical locations where classified communication will be needed. Additionally, the wireless capability reduces the traveling weight of the unit and reduces the complexity and durations of the setup operations in new locations.

ABOUT PERATON LABS

At Peraton Labs, we invent, advance, and mature new technologies, applying them to real-world problems to create novel, breakthrough solutions for our customers' most difficult challenges. As part of Peraton, we deliver trusted and highly differentiated national security solutions and technologies that keep people safe and secure.

For more information on our CSfC integration services, see CSfC trusted integrator - Peraton Labs or contact the Peraton Labs CSfC experts at trusted.csfc@peratonlabs.com.

Peraton